Given name:_____ **Family name:**_____

Student number:_____ **Signature:**_____

UNIVERSITY OF TORONTO
Faculty of Arts and Science

MAT 315H1S (Introduction to Number Theory)
Instructor: Yuri Burda

Midterm
February 28, 2012

Duration: 3 hours

No aids allowed

This examination paper consists of **9** pages and **5** questions. Please bring any discrepancy to the attention of an invigilator. The number in brackets at the start of each question is the number of points the question is worth.

Answer all questions.

To obtain credit, you must give arguments to support your answers.

For graders' use:

	Score
1 (15)	
2 (15)	
3 (20)	
4 (30)	
5 (20)	
Total (100)	

1. [15] Find a parametrization of all the rational solutions (x, y) of the equation

$$5x^2 - y^2 = 1$$

2. [15]

Alice thinks of a natural number between 1 and 100 and tells that after multiplying this number by 71 she gets an answer ending in 53. What answer did Alica get?
(*hint: first find what number Alice thought of originally*)

3. (a) [10] Let $x_1, \ldots, x_7$ be all the different solutions modulo 43 of the congruence $x^7 \equiv 1 \mod 43$. Find

$$x_1^5 + x_2^5 + \ldots + x_7^5 \mod 43$$

(b) [10] Find the number of solutions of the congruence

$$1 + x + x^2 + \ldots + x^{24} \equiv 0 \mod 11 \cdot 41$$

4. (a) [8] Find the last three digits of 3^{400000}

(b) [8] Find the last three digits of 3^{399998}

(c) [7] Find the last three digits of 2^{400000}

(d) [7] Find the last three digits of $2^{\left(2^{200002}\right)}$

5. (a) [10] Suppose that $p = \frac{3^n-1}{2}$ is a prime, where $n \geq 3$ is an integer.

   i. Show that n is odd.

   ii. Show that $2n$ divides $p - 1$.

(b) [10] Suppose that 8 is a primitive root modulo a prime $p > 3$. Show that $p \equiv -1 \mod 3$.

Total pages: 9